

Entanglement Enhances Security in Secret Sharing

Rafał Demkowicz-Dobrzański¹, Aditi Sen(De)³, Ujjwal Sen³, Maciej Lewenstein^{2,3}

¹*Institute of Physics, Nicolaus Copernicus University, ul. Grudziadzka 5, 87-100 Toruń, Poland*

²*ICREA and ³ICFO-Institut de Ciències Fotòniques, E-08860 Castelldefels (Barcelona), Spain*

We analyze tolerable quantum bit error rates in secret sharing protocols, and show that using entangled encoding states is advantageous in the case when the eavesdropping attacks are local. We also provide a criterion for security in secret sharing – a parallel of the Csiszár-Körner criterion in single-receiver cryptography.

In the last few years, the role of entanglement in different branches of physics has been studied extensively, ranging from many-body physics [1, 2] to quantum information processing [3]. In particular, the qualities and thresholds of entanglement for optimal quantum communication performance have been found, e.g. with regard to teleportation [4], dense coding [5], and cryptography [6]. The necessity of entanglement in quantum computation is still under investigation (see e.g. [7]). In a different context, there is an ongoing research on the behavior of entanglement in e.g. quantum phase transitions [2], local cloning [8], and local state distinguishing [9].

In this paper, we will investigate the advantage of entanglement in the security of a quantum communication task, known as secret sharing [10, 11], which is a communication scenario in which a sender Alice (A) wants to provide a (classical) message to two recipients (Bobs – B_1, B_2), in a way that each of the Bobs individually knows nothing about the message, but they can recover its content once they cooperate. In order to transmit a binary message string $\{a_i\}$, Alice can then take a sequence of completely random bits $\{b_{1,i}\}$, send it to B_1 , and at the same time send a sequence $\{b_{2,i}\} = \{a_i \oplus b_{1,i}\}$ to B_2 , where \oplus denotes addition modulo 2. Thus $a_i = b_{1,i} \oplus b_{2,i}$, assuring that the Bobs can recover the message if they cooperate, and yet none of them can learn anything on the message of Alice on his own, since the sequences $\{b_{1,i}\}$, $\{b_{2,i}\}$ are completely random.

An important issue is of course security, i.e. distributing the message in a way that no third (actually fourth!) party learns about it. This can be achieved using quantum cryptography (e.g. by the BB84 scheme [12]). Alice simply has to establish secret random keys, independently, with both Bobs, and use them as one-time pads to securely send bits in the way required by secret sharing. We call this the BB84^{⊗2} protocol. It has been argued [10] that a more natural way of using quantum states in secret sharing is to send entangled states to the Bobs, and as a result, avoid establishing random keys with each of the Bobs separately, by combining the quantum and classical parts of secret sharing in a single protocol. We call the protocol in [10, 11] as E4 (since it uses four entangled states).

In this paper, we consider security thresholds for both E4 and BB84^{⊗2}, i.e. the highest quantum bit error rates

(QBERs) below which one-way distillation of secret key is possible. There are three main results proven in the paper. *First*, we provide a criterion for security of secret sharing, for which one-way classical distillation of secret key is possible between the sender and the receivers: the parallel of the Csiszár-Körner criterion in (single-receiver, classical) cryptography [13]. *Secondly*, we find the *optimal* quantum eavesdropping attacks on both E4 and BB84^{⊗2}, that are individual, without quantum memory, and most importantly, *local*. Note that an attack which acts by local operations and classical communication (LOCC) on the particles sent through the two channels ($A \rightarrow B_1$ and $A \rightarrow B_2$) is physically more relevant in this distributed receivers case. We show that the threshold QBER for E4 is about 18.2 % higher than that of BB84^{⊗2}. This shows, to our knowledge for the first time, that it is more secure to use entangled encoding states in secret sharing. *Thirdly*, we provide an interesting general method for dealing with local eavesdropping attacks.

The protocols. In our setting, a secret sharing protocol can be characterized by $\{|\psi^{j,0}\rangle, |\psi^{j,1}\rangle, \sigma_1^{j,k} \otimes \sigma_2^{j,k}\}$, where j labels the different encoding “bases” used, $|\psi^{j,a}\rangle$ are two-qubit states sent by Alice to the Bobs if she uses basis j and wants to communicate the logical value a , while $\sigma_1^{j,k} \otimes \sigma_2^{j,k}$ is a set of observables compatible with basis j (so that if the corresponding measurement is performed by the Bobs, it allows them to recover a proper logical bit of Alice). In practice, B_1 (B_2) randomly measures the observables $\sigma_1^{j,k}$ ($\sigma_2^{j,k}$) on states received from Alice in each round. After the transmission is completed, the Bobs announce the observables they have used in each round to Alice, who, judging on whether this combination of observables is present in $\sigma_1^{j,k} \otimes \sigma_2^{j,k}$ for the particular j she had used in that round, tells the Bobs whether to keep or reject their measured results for that round – this is called the sifting phase. The BB84^{⊗2} protocol is defined as

j	$ \psi^{j,0}\rangle$	$ \psi^{j,1}\rangle$	$\sigma_1^{j,k} \otimes \sigma_2^{j,k}$
1	$ x_+\rangle x_+\rangle, x_-\rangle x_-\rangle$	$ x_+\rangle x_-\rangle, x_-\rangle x_+\rangle$	$\sigma_x \otimes \sigma_x$
2	$ x_+\rangle y_+\rangle, x_-\rangle y_-\rangle$	$ x_+\rangle y_-\rangle, x_-\rangle y_+\rangle$	$\sigma_x \otimes \sigma_y$
3	$ y_+\rangle x_+\rangle, y_-\rangle x_-\rangle$	$ y_+\rangle x_-\rangle, y_-\rangle x_+\rangle$	$\sigma_y \otimes \sigma_x$
4	$ y_+\rangle y_+\rangle, y_-\rangle y_-\rangle$	$ y_+\rangle y_-\rangle, y_-\rangle y_+\rangle$	$\sigma_y \otimes \sigma_y$

where $|x_{\pm}\rangle$ ($|y_{\pm}\rangle$) are eigenstates of the Pauli σ_x (σ_y)

matrix. The fact that there are two states corresponding to a given $|\psi^{j,a}\rangle$ simply means that each of them is sent randomly with probability $1/2$. The E4 protocol [10] (see also [15]), on the other hand, is defined as

$$\begin{array}{c|c|c} j & |\psi^{j,0}\rangle & |\psi^{j,1}\rangle & \sigma_1^{j,k} \otimes \sigma_2^{j,k} \\ \hline 1 & |\psi_+\rangle & |\psi_-\rangle & \sigma_x \otimes \sigma_x, \quad -\sigma_y \otimes \sigma_y \\ 2 & |\psi_+^i\rangle & |\psi_-^i\rangle & \sigma_x \otimes \sigma_y, \quad \sigma_y \otimes \sigma_x, \end{array}$$

where $|\psi_\pm\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2}$, $|\psi_\pm^i\rangle = (|00\rangle \pm i|11\rangle)/\sqrt{2}$, and $|0\rangle, |1\rangle$ are eigenstates of the Pauli σ_z operator. The question is which of these protocols tolerates a higher QBER. After the sifting phase, let the bits of Alice and the Bobs, obtained in a given set of rounds, be described by the probability distribution $p_{AB_1B_2}(a, b_1, b_2)$. The corresponding QBER is $\text{QBER} = \sum_{a,b_1,b_2} p_{AB_1B_2}(a, b_1, b_2)[1 - \delta_{a,b_1 \oplus b_2}]$.

Error correction and privacy amplification. Knowing QBER, we want to perform an one-way error correction procedure, such that all errors are corrected with arbitrarily high probability. In standard (single-receiver) cryptography, error correction can be performed either from the sender to the receiver, or vice-versa. In secret sharing, there are two *separated* receivers, and each of them individually has bits that are completely random. So there is no way for Alice to perform one-way error correction to Bobs – whatever she sends to each of them individually, it will not be enough for them to correct errors, unless she sends the total information which is of course not the solution we are after.

The only remaining option is that each of Bobs sends some information to Alice, judging on which she is able to correct her bits $\{a_i\}$ in a way that for every i : $a_i = b_{1,i} \oplus b_{2,i}$. Fortunately, this is indeed possible. We present here an idea how this can be achieved. We will adapt for our needs, a standard method in classical communication theory – namely, that of random coding (see e.g. [16, 17, 18]). Let each of the three parties have n bits after the sifting phase. The error correction procedure uses a random coding function $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$, known to all three parties (and the rest of the world), where $m \leq n$ will be chosen later. This function assigns a random m -bit codeword to each of 2^n possible n -bit strings. Error correction goes as follows: B_1 and B_2 calculate $f(\{b_{1,i}\})$ and $f(\{b_{2,i}\})$ respectively, and send their m -bit codewords to Alice. After this, Alice looks for all n -bit sequences $\{b'_{1,i}\}, \{b'_{2,i}\}$ such that $f(\{b'_{1,i}\}) = f(\{b_{1,i}\})$, $f(\{b'_{2,i}\}) = f(\{b_{2,i}\})$, and chooses a pair $\{b'_{1,i}\}, \{b'_{2,i}\}$, for which the Hamming distance $\text{dist}(\{a_i\}, \{b'_{2,i} \oplus b'_{1,i}\})$ is minimal. It can be shown that in the limit $n \rightarrow \infty$, this strategy is successful with arbitrarily high probability, provided

$$m \geq n[1 + h(\text{QBER})]/2, \quad (1)$$

where $h(p) = -p \log_2 p - (1-p) \log_2 (1-p)$ is the binary entropy function. This result is quite intuitive, since in a

standard bipartite error correction, the length of a codeword has to fulfill $m \geq nh(\text{QBER})$. In secret sharing however, the two Bobs together have to provide Alice with $nh(\text{QBER}) + n$ bits. These additional n bits are needed, since a sequence of one of Bobs taken separately is completely random for Alice. As a result each of Bobs has to send a code of length given by Eq. (1).

After the error correction stage is completed, Alice and the Bobs need to perform privacy amplification, in order to obtain a possibly shortened, but a completely secure key, on which an eavesdropper has no information. Privacy amplification presents no additional difficulty in a secret sharing scenario, as compared to standard bipartite cryptography, since its performance, in principle, requires no additional communication between Alice and the Bobs. It is enough that all parties apply the same hashing function [14] for shortening the key, and if there were no errors, in the sense that for all i , $a_i = b_{1,i} \oplus b_{2,i}$, then there will be no errors in the shortened key.

LOCC attacks. We will analyze security of the protocols with the following restrictions imposed on an eavesdropper: (i) Eavesdropper can perform only individual attacks; (ii) Individual attacks are LOCC operations with respect to partition of the encoding states between B_1 and B_2 ; (iii) Eavesdropper is not allowed any kind of quantum memory. The restriction (i) means that an eavesdropper can interact, in a given round, with only the quantum state sent by Alice to Bobs in that round. Restriction (ii) is at the heart of the problem we analyze, and is natural in the distributed receivers scenario. Note here that if no LOCC condition is imposed, then the security analyses of the two-receiver E4 and single-receiver BB84 protocols are isomorphic. The justification of (iii) is based on current technology limitations – no long lasting quantum memory has been developed so far.

Let the probability distribution $p_{ABE}(a, b, e)$ describe single-round bit values, a of Alice, $b = b_1 \oplus b_2$ of the Bobs, and e of an eavesdropper, after the eavesdropper's attack and after the sifting stage is completed. In single-receiver cryptography, the maximal one-way secret key distillation rate K is given by the Csiszár-Körner criterion [13]: $K = I(A : B) - \min(I(A : E), I(B : E))$, where $I(\cdot : \cdot)$ is the mutual information between the corresponding parties. As discussed in previous paragraphs, error correction in secret sharing can be performed only in one direction (from Bobs to Alice). Thus the secret key distillation rate in case of secret sharing is $K = I(A : B) - I(B : E)$, which is therefore the parallel of the Csiszár-Körner criterion in (single-receiver) cryptography [13].

In order to analyze eavesdropping attacks, consider the state $|\psi^{j,a}\rangle$ being sent from Alice to Bobs. Collaborating eavesdroppers E_1, E_2 , acting on channels connecting A with B_1 and B_2 respectively, can perform an arbitrary LOCC operation \mathcal{E} (completely positive trace-preserving LOCC map) to create $\rho_{B_1B_2E_1E_2}^{j,a} = \mathcal{E}(|\psi^{j,a}\rangle\langle\psi^{j,a}|)$. The operation is LOCC with respect to the partition

$B_1, E_1 \mid B_2, E_2$. Subsequently, E_1, E_2 perform an LOCC measurement on their subsystems in order to obtain information about the bit shared by Alice with Bobs, while sending possibly-perturbed subsystems B_1, B_2 to their legitimate recipients. Without loosing generality, we can restrict this measurement to have only two possible outcomes (0 or 1), since only the value of a transmitted bit is of interest to the eavesdroppers. Hence we model the measurement by a two element positive operator valued measurement (POVM): $\Pi_{E_1 E_2}(0), \Pi_{E_1 E_2}(1)$. Obviously $\Pi_{E_1 E_2}(e) \geq 0$, and $\Pi_{E_1 E_2}(0) + \Pi_{E_1 E_2}(1) = \mathbb{1}_{E_1 E_2}$, but here we additionally impose the constraint that the measurements are LOCC-based.

The probability distribution $p_{ABE}(a, b, e)$ is given by $\sum_j p(j, a) \text{Tr}[\mathcal{E}(|\psi^{j,a}\rangle\langle\psi^{j,a}|) \Pi_{B_1 B_2}(j, b) \otimes \Pi_{E_1 E_2}(e)]$, where $p(j, a)$ is the probability that A sends the state $|\psi^{j,a}\rangle$ in a given round, whereas $\{\Pi_{B_1 B_2}(j, b)\}$ is a POVM corresponding to Bobs' measurement in basis j (compatible with the state sent by Alice), where the sum of their individual measured values, modulo 2, is equal b : $b = b_1 \oplus b_2$. Probability normalization condition reads $\Pi_{B_1 B_2}(j, 0) + \Pi_{B_1 B_2}(j, 1) = \mathbb{1}_{B_1 B_2}$. We assume the convention that if one of Bobs (locally) performs a measurement characterized by a Pauli matrix σ_i , then he ascribes the bit value 0 or 1, once in a measurement he projects on an eigenvector with eigenvalue -1 or 1 respectively. To make $p_{ABE}(a, b, e)$ more revealing, we introduce non-trace-preserving completely positive operations $\mathcal{E}_0, \mathcal{E}_1 : \mathcal{H}_{B_1}^{\text{in}} \otimes \mathcal{H}_{B_2}^{\text{in}} \mapsto \mathcal{H}_{B_1}^{\text{out}} \otimes \mathcal{H}_{B_2}^{\text{out}}$ acting on the input and output Hilbert spaces of the Bobs, and defined as $\mathcal{E}_e(\varrho_{B_1 B_2}) = \text{Tr}_{E_1 E_2}[\mathcal{E}(\varrho_{B_1 B_2}) \Pi_{E_1 E_2}(e)]$. \mathcal{E}_e represents the disturbance experienced by a state transmitted to the Bobs, once the eavesdroppers have obtained a particular value e in their measurement. Notice that even though each operation \mathcal{E}_e is not trace-preserving the operation $\mathcal{E}_0 + \mathcal{E}_1$ is – it corresponds to a situation when one averages over the results of the eavesdroppers' measurement. We can now write $p_{ABE}(a, b, e) = \sum_j p(j, a) \text{Tr}[\mathcal{E}_e(|\psi^{j,a}\rangle\langle\psi^{j,a}|) \Pi_{B_1 B_2}(j, b)]$. It is now clear, that the eavesdropping strategy is completely defined by specifying the two operations $\mathcal{E}_0, \mathcal{E}_1$, and for a given protocol yields a joint probability distribution $p_{ABE}(a, b, e)$.

To calculate the QBER threshold, one should now look for the highest value of QBER, for which it is still possible to find eavesdropping LOCC operations \mathcal{E}_e , so that the resulting probability distribution p_{ABE} enjoys the property $I(A : B) = I(B : E)$. Forgetting for the moment about the LOCC constraint, the problem of finding the QBER threshold is a semi-definite program. To see this, let us denote $\mathcal{H}^{\text{out}} = \mathcal{H}_{B_1}^{\text{out}} \otimes \mathcal{H}_{B_2}^{\text{out}}$, $\mathcal{H}^{\text{in}} = \mathcal{H}_{B_1}^{\text{in}} \otimes \mathcal{H}_{B_2}^{\text{in}}$ and recall the Jamiołkowski isomorphism [19] between completely positive maps \mathcal{E}_e and positive semi-definite operators $P_{\mathcal{E}_e} \in \mathcal{L}(\mathcal{H}^{\text{out}} \otimes \mathcal{H}^{\text{in}})$: $P_{\mathcal{E}_e} = \mathcal{E}_e \otimes \mathcal{I}(|\Psi^+\rangle\langle\Psi^+|)$, where $|\Psi^+\rangle = \sum_{i=1}^{\dim \mathcal{H}^{\text{in}}} |i\rangle \otimes |i\rangle$ is an unnormalized maximally entangled state in the space $\mathcal{H}^{\text{in}} \otimes \mathcal{H}^{\text{in}}$, and \mathcal{I} is an

identity operation on \mathcal{H}^{in} . Hence our problem variables are entries of two 16×16 matrices, which are required to be positive semi-definite. Trace-preservation condition of $\mathcal{E}_0 + \mathcal{E}_1$ translates to a condition on positive operators: $\text{Tr}_{\mathcal{H}^{\text{out}}}(P_{\mathcal{E}_0} + P_{\mathcal{E}_1}) = \mathbb{1}_{\mathcal{H}^{\text{in}}}$. This condition is obviously linear in the matrix elements of $P_{\mathcal{E}_e}$. Similarly, p_{ABE} is also linear, and hence the security condition is linear. Finally, the QBER, which we want to maximize, is linear. In order to deal with an LOCC constraint, we will impose the weaker ‘‘PPT constraint’’: positivity after partial transposition of the $P_{\mathcal{E}_e}$ operators – we transpose subsystem $\mathcal{H}_{B_2}^{\text{out}} \otimes \mathcal{H}_{B_2}^{\text{in}}$. This is a strictly necessary condition for LOCC [20]. However, we will show that the optimal PPT maps are also LOCC.

Entangled vs. product encoding. We now present the solutions for maximal tolerable QBER for BB84^{⊗2} and E4 protocols found by solving the corresponding semi-definite programs, using the SeDuMi package. Although solving a semi-definite program provided us only with numerical solutions, we were able to recognize their analytical form, and hence all results presented are analytical.

For the BB84^{⊗2} protocol, the optimal $P_{\mathcal{E}_0^{\text{BB84}^{\otimes 2}}}$, in the computational basis, = $\frac{1}{18} \text{diag}[4, 2, 2, 1, 2, 4, 1, 2, 2, 1, 4, 2, 1, 2, 2, 4]$ + the 16×16 matrix $(\alpha_{i,j})$ whose only nonzero elements are $\alpha_{1,4} = \alpha_{5,8} = \alpha_{5,12} = \alpha_{9,12} = \alpha_{13,16} = \alpha_{1,13}^* = \alpha_{2,14}^* = \alpha_{2,15}^* = \alpha_{3,14}^* = \alpha_{3,15}^* = \alpha_{4,16}^* = \alpha_{8,9}^* = i/9$, $\alpha_{1,16} = \alpha_{6,11} = 2/9$, $\alpha_{2,3} = \alpha_{5,9} = \alpha_{6,7} = \alpha_{6,10} = \alpha_{7,11} = \alpha_{8,12} = \alpha_{10,11} = \alpha_{14,15} = 1/9$, $\alpha_{7,10} = -\alpha_{4,13} = 1/18$, and hermitian conjugates. The optimal $P_{\mathcal{E}^{\text{BB84}^{\otimes 2}}}$ has the same entries on the diagonal, and the anti-diagonal, while the remaining ones are multiplied by -1 . These optimal PPT maps will later on proven to be LOCC. The optimal $\text{QBER}(\text{BB84}^{\otimes 2}) = 5/18 \approx 0.2778$.

Moving now to the E4 protocol, the optimal $P_{\mathcal{E}_0^{\text{E4}}}$ = $\text{diag}[a, b, b, d, b, a, d, b, b, d, a, b, d, b, b, a]$ + the 16×16 matrix $(\beta_{i,j})$ whose only nonzero entries are $\beta_{1,4} = \beta_{1,13}^* = \beta_{4,16}^* = \beta_{13,16} = c$, $\beta_{1,16} = a$, $\beta_{4,13} = f^*$, and the hermitian conjugates, where $a = 3 - 2\sqrt{2}$, $b = a/\sqrt{2}$, $c = b \exp(i\pi/4)$, $d = a/2$, $f = id$. The optimal $P_{\mathcal{E}_1^{\text{E4}}}$ is the same as $P_{\mathcal{E}_0^{\text{E4}}}$, but with c replaced by $-c$. Again these optimal PPT maps will later on proven to be LOCC. The optimal $\text{QBER}(\text{E4}) = 2(\sqrt{2} - 5/4) \approx 0.3284$. Interestingly therefore, $\text{QBER}(\text{E4})$ is about 18.2 % higher than $\text{QBER}(\text{BB84}^{\otimes 2})$, which indicates that indeed the protocol using entangled states is more secure, in the case of LOCC eavesdropping. In Fig.1, we show the maximum achievable secret-key rates for the two protocols as a function of measured QBER. It is clear that E4 is better not only because of its higher QBER threshold, but because of its higher key rate for all QBER (see Fig. 1, more details will be presented elsewhere [21])

Explicit LOCC forms of the optimal attacks. We now show that the optimal attacks are separable. We will

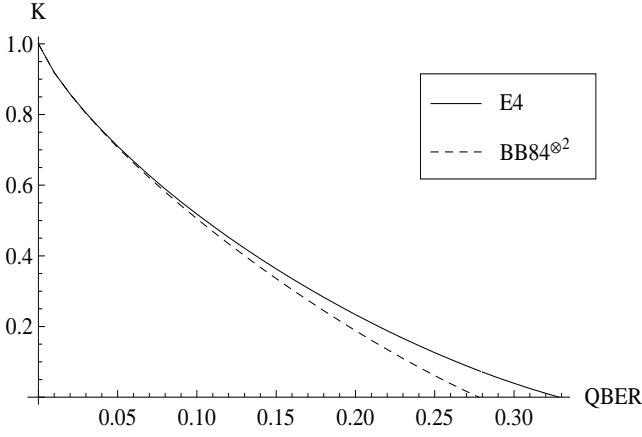


FIG. 1: Maximal achievable secret-key rates $K = I(A : B) - I(B : E)$ for E4 and $\text{BB84}^{\otimes 2}$, against local attacks.

subsequently show that the attacks are actually LOCC.

Separability of the optimal attack for the $\text{BB84}^{\otimes 2}$ case is evident once we write it in the form (the procedure leading to this form will be presented elsewhere [21])

$$\mathcal{E}_e^{\text{BB84}^{\otimes 2}}(\rho) = \sum_{\phi_1, \phi_2 \in \{0, \pi\}} K_{e, B_1}^{\phi_1, \phi_2} K_{e, B_2}^{\phi_1, \phi_2} \rho K_{e, B_1}^{\phi_1, \phi_2 \dagger} K_{e, B_2}^{\phi_1, \phi_2 \dagger},$$

where the local Kraus operators $K_{e, B_1}^{\phi_1, \phi_2}$, $K_{e, B_2}^{\phi_1, \phi_2}$ are

$$\frac{1}{\sqrt{6}} \begin{bmatrix} (-1)^e \sqrt{2} & \exp[i(\phi_1 - \pi/4)] \\ \exp[i(\phi_2 + \pi/4)] & (-1)^e \sqrt{2} \exp[i(\phi_1 + \phi_2)] \end{bmatrix},$$

$$\frac{1}{2\sqrt{3}} \begin{bmatrix} \sqrt{2} & \exp[-i(\phi_1 + \pi/4)] \\ \exp[-i(\phi_2 - \pi/4)] & \sqrt{2} \exp[i(\phi_1 + \phi_2)] \end{bmatrix}$$

respectively. Since K_{e, B_2} does not depend on e (equivalently, K_{e, B_1} can also be chosen to be so), we write it as K_{B_2} . The full operation $\mathcal{E}^{\text{BB84}^{\otimes 2}} = \mathcal{E}_0^{\text{BB84}^{\otimes 2}} + \mathcal{E}_1^{\text{BB84}^{\otimes 2}}$ can be written as $\sum_{\phi_1, \phi_2 \in \{0, \pi\}} \mathbb{1} \otimes K_{B_2}^{\phi_1, \phi_2} (\sum_{e=0}^1 K_{e, B_1}^{\phi_1, \phi_2} \otimes \mathbb{1} \rho K_{e, B_1}^{\phi_1, \phi_2 \dagger} \otimes \mathbb{1}) \mathbb{1} \otimes K_{B_2}^{\phi_1, \phi_2 \dagger}$, which shows that it is indeed LOCC, since it can be realized as follows. First an operation given by the four Kraus operators $K_{B_2}^{\phi_1, \phi_2}$ is performed on the second subsystem, and the measurement result (ϕ_1, ϕ_2) is transmitted to the first subsystem. For given values of (ϕ_1, ϕ_2) received by the first subsystem, an operation using the two Kraus operators $K_{0, B_1}^{\phi_1, \phi_2}$, $K_{1, B_1}^{\phi_1, \phi_2}$ is performed on the first subsystem. This is a legitimate deterministic LOCC operation since $\sum_{\phi_1, \phi_2 \in \{0, \pi\}} K_{B_2}^{\phi_1, \phi_2 \dagger} K_{B_2}^{\phi_1, \phi_2} = \mathbb{1}$, and for every (ϕ_1, ϕ_2) , $\sum_{e=0}^1 K_{e, B_1}^{\phi_1, \phi_2 \dagger} K_{e, B_1}^{\phi_1, \phi_2} = \mathbb{1}$. Note that it requires only one-way classical communication. Summing up, $\mathcal{E}_e^{\text{BB84}^{\otimes 2}}$ are separable trace-decreasing operations, such that when added together, they form a trace-preserving LOCC operation $\mathcal{E}^{\text{BB84}^{\otimes 2}}$, and hence they can both be realized via LOCC.

In a similar way, we can show that the optimal PPT attacks on the E4 protocol are also LOCC. Separable Kraus decompositions of $\mathcal{E}_e^{\text{E4}}$ read

$$\mathcal{E}_e^{\text{E4}}(\rho) = \sum K_{e, B_1}^{\phi_1, \phi_2, \phi_3} K_{B_2}^{\phi_1, \phi_2, \phi_3} \rho K_{e, B_1}^{\phi_1, \phi_2, \phi_3 \dagger} K_{B_2}^{\phi_1, \phi_2, \phi_3 \dagger},$$

where the sum runs over $\phi_1, \phi_2, \phi_3 \in \{0, 2\pi/3, 4\pi/3\}$, and $K_{e, B_1}^{\phi_1, \phi_2, \phi_3}$, $K_{e, B_2}^{\phi_1, \phi_2, \phi_3}$ are respectively

$$\sqrt{1 + \frac{1}{\sqrt{2}}} \begin{bmatrix} (-1)^e 2^{1/4} & \exp(i\phi_1) \\ \exp(i\phi_2) & (-1)^e 2^{1/4} \exp(i\phi_3) \end{bmatrix},$$

$$\frac{1}{\sqrt{27(1 + \sqrt{2})}} \begin{bmatrix} 2^{1/4} & \exp[-i(\phi_1 + \pi/4)] \\ \exp[-i(\phi_2 - \pi/4)] & 2^{1/4} \exp(-i\phi_3) \end{bmatrix}.$$

Again we can write the full operation $\mathcal{E}^{\text{E4}} = \mathcal{E}_0^{\text{E4}} + \mathcal{E}_1^{\text{E4}}$ as $\sum_{\phi_1, \phi_2, \phi_3 \in \{0, 2\pi/3, 4\pi/3\}} \mathbb{1} \otimes K_{B_2}^{\phi_1, \phi_2, \phi_3} (\sum_{e=0}^1 K_{e, B_1}^{\phi_1, \phi_2, \phi_3} \otimes \mathbb{1} \rho K_{e, B_1}^{\phi_1, \phi_2, \phi_3 \dagger} \otimes \mathbb{1}) \mathbb{1} \otimes K_{B_2}^{\phi_1, \phi_2, \phi_3 \dagger}$, which shows that it is an LOCC, since it can be realized by performing an operation on the second subsystem using the 27 Kraus operators $K_{B_2}^{\phi_1, \phi_2, \phi_3 \dagger}$, communicating the measurement result (ϕ_1, ϕ_2, ϕ_3) to the first subsystem, on which an appropriate operation using the two Kraus operators $K_{e, B_1}^{\phi_1, \phi_2, \phi_3}$ ($e = 0, 1$) is performed. Note that $\sum_{\phi_1, \phi_2, \phi_3 \in \{0, 2\pi/3, 4\pi/3\}} K_{B_2}^{\phi_1, \phi_2, \phi_3 \dagger} K_{B_2}^{\phi_1, \phi_2, \phi_3} = \mathbb{1}$, and for every (ϕ_1, ϕ_2, ϕ_3) , $\sum_{e=0}^1 K_{e, B_1}^{\phi_1, \phi_2, \phi_3 \dagger} K_{e, B_1}^{\phi_1, \phi_2, \phi_3} = \mathbb{1}$.

Typical noise. Judging the usefulness of the two protocols by comparing their QBER thresholds, may apriori be not sensible from an experimental point of view, as in an experiment, we face noise caused by natural factors, as well as by the eavesdropper. Hence a relevant question is: Which protocol allows a secure key transmission in presence of a higher level of noise, of the type present in an experiment? Consider a typical situation when we send the qubits via two fibers. A usual model of noise here would be that each channel (fiber) is an isotropically depolarizing channel – and they are independent. Given a channel with a fixed level of depolarization, we ask: Can we securely extract some secret key using either the E4 or the $\text{BB84}^{\otimes 2}$ protocol? This may not be equivalent to comparing QBER thresholds, because different states are used in the two protocols, which under the same noise level, may behave differently, and result in different QBERs – in particular it could happen that in such situation it might be advantageous to apply a protocol with lower QBER threshold. In this environment, however, the QBERs for E4 and $\text{BB84}^{\otimes 2}$ depend in the same way on the depolarization parameter. If an isotropically depolarizing qubit channel acts as $\mathcal{D}(\rho) = (1 - p)\rho + p\mathbb{1}/2$, then the QBER caused by the $\mathcal{D}^{\otimes 2}$ channel is $\text{QBER} = p(1 - p/2)$ for *both* the protocols. Comparing protocols using QBER thresholds as a figure of merit is legitimate both from theoretical and practical point of view.

Summary. We have for the first time shown that entanglement in the encoding states provide a better security in secret sharing. The security was judged by calculating QBER threshold for secure communication, under assumption of local individual quantum attacks without quantum memory. We have found the optimal attacks in such scenario for the two paradigmatic protocols: one using product states and the other using entangled ones for encoding. Further results include the parallel of the Csiszár-Körner criterion for security in (single-receiver) cryptography in the distributed-receivers case, and usefulness of the protocols in the presence of a depolarizing environment.

We acknowledge support from the Spanish MEC (FIS-2005-04627, Consolider QOIT, Acciones Integradas, & Ramón y Cajal), ESF Program QUDEDIS, Euroquam FERMIX, Polish Ministry of Science and Higher Education grant no. 1 P03B 011 29, EU IP SCALA, EU IP QAP.

-
- [1] M. Lewenstein *et al.*, Adv. Phys. **56**, 243 (2007).
 - [2] L. Amico *et al.*, to appear in Rev. Mod. Phys. (quant-ph/0703044).
 - [3] R. Horodecki *et al.*, to appear in Rev. Mod. Phys. (quant-ph/0702225).
 - [4] See e.g. C.H. Bennett *et al.*, Phys. Rev. Lett. **70**, 1895 (1993); P. Horodecki, M. Horodecki, and R. Horodecki, Phys. Rev. A **60**, 1888 (1999).
 - [5] C.H. Bennett and S.J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
 - [6] See e.g. A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991); N. Gisin *et al.*, Rev. Mod. Phys. **74**, 145 (2002); K. Horodecki *et al.*, *ibid.* **94**, 160502 (2005).
 - [7] A. Datta and G. Vidal, Phys. Rev. A **75**, 042310 (2007).
 - [8] See e.g. R. Demkowicz-Dobrzański *et al.*, Phys. Rev. A **73**, 032313 (2006).
 - [9] See e.g. M. Hayashi *et al.*, Phys. Rev. Lett. **96**, 040501 (2006).
 - [10] M. Żukowski, A. Zeilinger, M. Horne, and H. Weinfurter, Acta Phys. Pol. **93**, 187 (1998); M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).
 - [11] R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999); A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999).
 - [12] C.H. Bennett and G. Brassard, in *Proceedings of the International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, NY (1984)).
 - [13] I. Csiszár and J. Körner, IEEE Trans. Inf. Th. **IT-24**, 339 (1978).
 - [14] C.H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, IEEE Trans. Inf. Theory, **41**, 1915 (1995).
 - [15] V. Scarani and N. Gisin, Phys. Rev. Lett. **87**, 117901 (2001); Phys. Rev. A **65**, 012311 (2002); A. Sen(De), U. Sen, and M. Żukowski, Phys. Rev. A **68**, 032309 (2003); C. Schmid *et al.*, Phys. Rev. Lett. **95**, 230505 (2005).
 - [16] T.M. Cover and J.A. Thomas, *Elements of Information Theory* (Wiley, NJ (1991)).
 - [17] G. Brassard and L. Salvail, Adv. Cryptol. **765**, 410 (1994).
 - [18] M.A. Nielsen and I.L. Chuang, *Quantum Computing and Quantum Information* (CUP, Cambridge (2000)).
 - [19] A. Jamiolkowski, Rep. Math. Phys. **3**, 275 (1972).
 - [20] P. Horodecki, Phys. Lett. A **232**, 333 (1997); M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998); C.H. Bennett *et al.*, Phys. Rev. A **59**, 1070 (1999).
 - [21] R. Demkowicz-Dobrzański, A. Sen(De), U. Sen, and M. Lewenstein, in preparation.